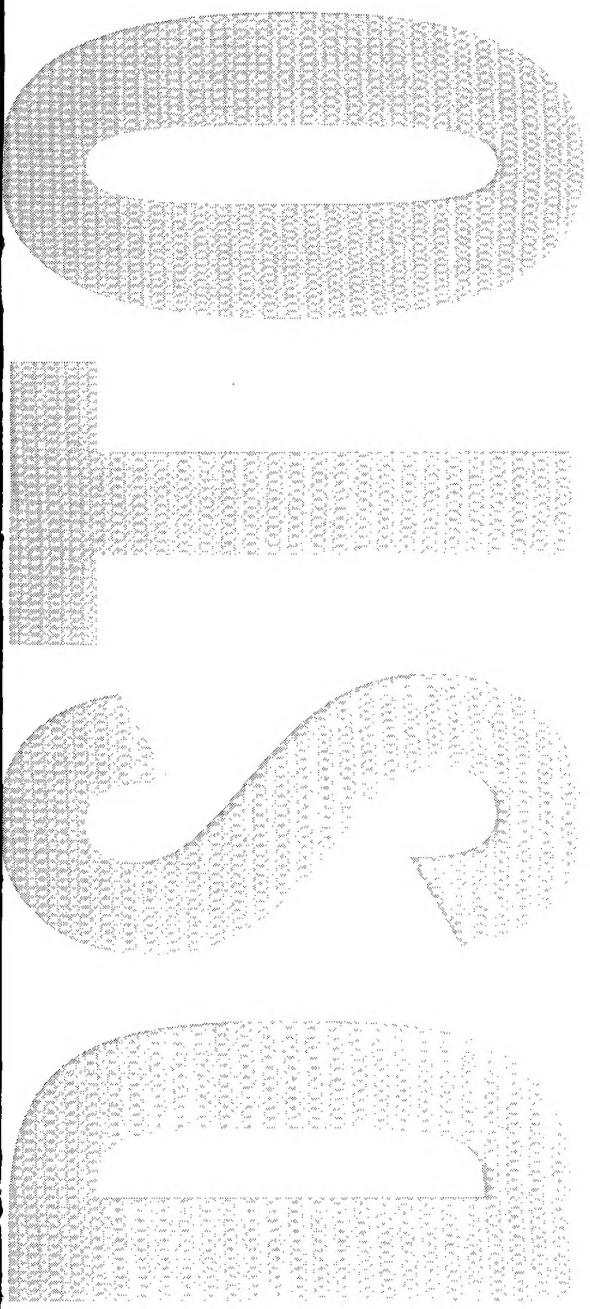
DEPARTMENT OF DEFENCE
DEFENCE SCIENCE & TECHNOLOGY ORGANISATION
DSTO



IP Convergence in Global Telecommunications

-

New Approaches to Network Management and Service Provision

Peter George and
Marek Kwiatkowski

DSTO-TR-1075

IP Convergence in Global Telecommunications
-
New Approaches to Network Management and Service Provision

Peter George and Marek Kwiatkowski

Communications Division
Electronics and Surveillance Research Laboratory

DSTO-TR-1075

ABSTRACT

This report overviews current and emerging approaches to network management and service provision in both voice and IP data public carrier networks. These two functions are described for the traditional infrastructure, where voice and data networks are separated, and when these networks are interconnected; the latter being an emerging trend.

DEPARTMENT OF DEFENCE
DEFENCE SCIENCE & TECHNOLOGY ORGANISATION
DSTO

Published by

DSTO Electronics and Surveillance Research Laboratory
PO Box 1500
Salisbury South Australia 5108 Australia

Telephone: (08) 8259 5555
Fax: (08) 8259 6567

AR-011-645
November 2000

APPROVED FOR PUBLIC RELEASE

IP Convergence in Global Telecommunications

-

New Approaches to Network Management and Service Provision

Executive Summary

This report overviews current and emerging approaches to network management and service provision in both voice and IP data public carrier networks. These two aspects of public network functioning are becoming of increasing importance due to the growing size and complexity of these networks, as well as the rapidly growing demand for new, sophisticated services.

The report first describes how network management and service provision are accomplished in traditional voice and IP data networks, presenting typical architectures and protocols. However, a new trend is emerging of joining separated voice and data public networks belonging to a single carrier into an integrated telecommunications infrastructure to provide highly innovative product packages.

The second part of the report provides an overview of some better-known new approaches to network management and service provision, which aim at coping with the complexity of joint voice/data infrastructures and providing mechanisms for rapid deployment of new services.

Contents

1. Introduction

Network management and service provision in today's public networks is becoming increasingly harder due to:

- Growing size of the networks as a result of increasing customer numbers;
- Growing complexity of the networks resulting from integrating previously separated voice and data networks, thus enabling connectivity between a broad range of end devices;
- Rapidly growing demand for new and increasingly sophisticated services, often involving various types of media.

The aim of this report is to briefly review current and emerging approaches to Network Management and Service Provision in public carrier networks. Following the ITU-T, the term *Network Management* is used in this report as a concept covering long-term activities including configuration management, fault management, performance management, accounting management and security management.

Service Provision (also known as Service Management) is related to activating, deactivating, suspending and resuming services across the network(s), as well as maintaining QoS (if used) of services according to Service Level Agreements (SLAs) between the network and the users. It is noted that Service Provision uses services provided by Network Management.

The structure of the report is as follows. Section 2 presents the way network management and service provision are accomplished in traditional voice and IP data networks. An overview of some better-known new approaches to network management and service provision, which aim at coping with the complexity of joint voice/data infrastructures and providing mechanisms for rapid deployment of new services, is described in Section 3.

2. Traditional Approaches to Network Management and Service Provision

2.1 Network Management

2.1.1 Public Voice Networks

Currently, network management in public voice networks is performed using a mixture of proprietary and standardised architectures and tools. As for the standardised architectures, these are usually based on the ITU-T *Telecommunications Management Network* (TMN) framework. It is noted that although it is a powerful framework, being already well standardised, it hasn't been fully implemented in voice

networks due to its complexity and slowly developing market of supportive management tools.

The TMN is based on the Open Systems Interconnections (OSI) management. It is a conceptual and technological framework that offers [1]:

- A set of *standardised interfaces,* designed to transfer management information between a TMN, being a conceptually separate subnetwork, and telecommunications network equipment, as well as between TMNs of cooperating networks;
- An object-oriented architecture, in which the physical and logical resources of a telecommunications network are viewed as objects that can be managed. The *Management Information Base* (MIB) is used as a repository of management objects;
- An *organisational model* using the *manager-agent* concept, where an agent accomplishes management operations on managed objects according to directives obtained from a manager, and returns results of those operations in the form of notifications.
- A management layer model, that supports the complex task of managing by splitting this task into different functions and placing them within the following layers:
  - The *Network Element Layer* (the lowest layer) is responsible for the management of particular *Network Elements* (NEs);
  - The *Network Element Management Layer* is used to control and coordinate groups of NEs;
  - The *Network Management Layer* performs control and coordination functions for all NEs which belong to the same carrier;
  - The *Service Management Layer* is involved in the control and management of services as well as in the interactions with service providers and customers subscribing services;
  - The *Business Management Layer* manages business aspects of the whole network.

  It is stressed that network management is covered by the lowest three layers of the model. On the other hand, service provision is performed in this architecture by the *Service Management Layer.*
- A *communication model,* that describes the functions, protocols and messages involved in exchange of information between TMN entities. The OSI protocol stack is used, with *Common Management Information Protocol* (CMIP) and *File Transfer Access and Management Protocol* (FTAM) being at the Application Layer. CMIP is a transaction-oriented protocol capable of invoking a rich set of operations on managed objects.

Below, some basic aspects of the TMN in relation to network management are presented.

Security

Until recently, only a modest degree of security could be achieved using TMN. It mainly allowed changing passwords, usually transferred in the clear [2]. However, there are new standardisation efforts to enhance TMN standards with the specification of security mechanisms, security transformation techniques (including evaluation of *Generic Upper Layer Security* (GULS) for TMN purposes) and management of security.

Robustness

TMN uses the connection-oriented CMIP protocol stack designed to cope with erroneous environments and losses of management messages. However, TMN, assuming a simple manager-agent relationship (a concept dating back to the mid-1980s), is not well suited to manage highly distributed (thus more robust) and dynamically reconfigurable networks [3]. In addition, adaptation of TMN to a changing environment is rather limited due to its lack of location transparency, requiring a manager to know the location of an agent (e.g. host address). That is why the ITU (jointly with ISO) has decided to extend the TMN model to include fully distributed management. This approach, called generic *Reference Model of Open Distributed Processing* (RM-ODP) is being utilised by the TINA project aiming at replacing the traditional ITU network control and management by a fully distributed architecture (see the next section).

Performance

The performance of TMN is satisfactory even for large networks. It can promptly react to network events due to the event-driven management (i.e., it does not require polling of network elements to obtain their status).

Scalability

TMN is well scalable by utilising hierarchical management and event-driven management. It enables creating both centralised and hierarchical management systems. However, the TMN lacks full support for distributed management [4].

Tools

Only recently the commercial world has started to offer tool kits supporting TMN operation. These include Hewlett-Packard's *OpenView* DM, IBM's *TMN WorkBench*, or DEC's *TeMIP*.

Complexity

One of TMN's big disadvantages is that its CMIP protocol is very complex to implement, requiring many more resources than other management protocols, such as the SNMP protocol presented in the next section.

2.1.2 IP data networks

Current management architectures for IP data networks are based on Simple Network Management Protocol (SNMP), which is used to manage routers and switches. It is noted that these networks are usually built on core infrastructure (e.g. SDH, ATM), which may be managed using other management systems, including proprietary and TMN solutions.

Network management in the Internet is composed of one or more *Network Management Stations* (NMSs) and one or more *Network Elements* (NEs). Like TMN, the Internet uses object orientated and manager-agent concepts. The managed objects are defined in the *Management Information Base* (MIB), which is different to the TMN MIB since objects in the Internet and those in OSI are different. The *Simple Network Management Protocol* (SNMP), a subset of CMIP, is used to transfer management information between an NMS and a NE. SNMP is a connection-less protocol and it has primarily been designed for environments with very low error rate, such as LANs and MANs. SNMP version 1 (SNMPv1) only supports centralised management systems (i.e. a single NMS manages a set of NEs), and it does not allow for bulk transfer of management information. SNMP version 2 (SNMPv2) additionally enables bulk transfers of management information (still rather poor when comparing with CMIP) and offers structured management supporting manager-to-manager cooperation. This version is widely supported within network equipment today. SNMP version 3 (SNMPv3) was approved as a draft standard in March 1999 and represents a convergence of the previous proposals (note that SNMPv2 had a number of variants), together with an attempt to provide a uniform security and management framework. Flexibility is the catch-cry of this framework, facilitating all versions of IP data management to coexist in a common architecture [5].

Some basic aspects of SNMP are presented below.

Security

Security is poorly supported by both SNMPv1 and SNMPv2. Version 3 (not yet standardised) will improve security through the use of authentication and access control [6]. As well as the framework for the access control and security subsystems, two initial core security models in each of those subsystems are proposed in version 3. Firstly the User-based Security Model (USM) [7] which provides for both Authenticated (using HMAC-MD5 and HMAC-SHA authentication protocols) and Private (using CBC-DEC encryption) SNMP messages. This addresses the security threats related to information modification, masquerading, confidentiality and message timeliness. It does not address the issues of denial-of-service or traffic analysis. Secondly, the View-based Access Control Model (VACM) [8] provides the ability to limit access to different MIB objects on a per-user basis. The mechanism to perform this function uses an extension to the concept of community strings. The agent has the responsibility to check whether a specific type of access to a specific managed object is allowed.

Under the new modular approach to the SNMPv3 framework, different security modules can coexistence. As an example, one security module may be based on SNMPv1 communities while the other uses a USM. It is also expected that new security or access control modules can and will be defined (e.g., use of IPSEC).

Robustness

SNMP is less robust than CMIP used by the TMN because it operates in a connectionless mode. In an erroneous environment, appropriate reliability of transferring management information can only be achieved by using retransmissions at the level of manager applications. On the other hand, SNMP is much simpler than CMIP, passing complexity to manager applications. Since SNMP uses the same manager-client model as TMN, its adaptation to changing environments is also rather limited.

Performance

SNMP is particularly well suited for LAN and MAN environments that are connectionless, where the available bandwidth is high and the error rate very low [9]. If this is the case, the performance of SNMP is better than using CMIP. However, in wide area networks with substantial error rate and limited bandwidth (e.g. satellite networks), polling status of network elements and the need for retransmissions may result in noticeable additional load.

Scalability

SNMP has been designed to allow management of networks containing a very large number of network elements. SNMP scales very well if the managed environment is characterised by a very low error rate (e.g. LANs/MANs). Otherwise, performance problems may be encountered (see above).

Tools

The management tools for SNMP are extensive and well supported. These tools include standalone tools (i.e. analysers), Management platforms, Integrating tools (i.e. enterprise management systems), and development tools (i.e. agent and MIB development).

Complexity

At the heart of SNMP's popularity is its simplicity and 'bare-bones' approach. While that could be said of earlier versions, some of the modules currently defined under version 3 are inherently complex to meet the growing needs of managing the emerging IP data networks.

2.2 Service Provision

2.2.1 Voice Networks

In voice networks, available services can be grouped as:

- Basic call services;
- Supplementary services, such as Closed User Group (CUG) service or redirection of a call;
- Intelligent Services, using the "intelligence" of *Service Control Points* (SCPs).

The Signalling System Number 7 (SS7) is used to control instances of these services in both the narrowband ISDN (ITU standard Q.931) and in broadband ATM networks (ITU standard Q.2931).

The deployment of new voice services is usually done using proprietary tools. It is a very rigid and time consuming (taking up to years) process. TMN, being designed to manage a large number of simple objects, is not well suited for service management [10]. To resolve this problem there are currently many attempts to integrate TMN network management with distributed processing environments such as CORBA (e.g. see [11,12,13]).

Lack of service management infrastructure leads to a very limited third-party involvement in services programming. The network operator has almost complete control over designing and implementing new services. Moreover, only a small number of operational parameters are usually customised. Such approaches were sufficient (and efficient) for simple, audio-only, two-party applications, but certainly not for future sophisticated multimedia/multiparty services.

2.2.2 IP Networks

As opposed to the ITU approach, the Internet technology relies largely on intelligence in user terminals. In the Internet, there is no strict distinction between network provider, service provider and user. Any user can be a service provider and network provider. This has been one of the most important features causing the enormous growth of this network. It is noted however, that in IP networks there is no support for fast deployment of network-based services and their automatic provisioning (e.g. VPNs automatically provisioned across an IP network).

3. New Trends in Network Management and Service Provision

3.1 General Remarks

A new trend is emerging of joining separated voice and data public networks, belonging to a single carrier, into a single telecommunications infrastructure to provide highly innovative product packages. In addition there is rapidly growing demand for new sophisticated services, often involving various types of media requiring quick deployment.

This section provides an overview of some better-known new approaches to network management and service provision, which aim at coping with the complexity of joint voice/data infrastructures and providing mechanisms to rapidly deploy new services.

3.2 Network Management

3.2.1 Telstra's DMO

If we examine Telstra's network management strategy under its emerging Data Mode of Operation (DMO) [14], we can find trends consistent with leading telecommunication providers in relation to migration towards a data/IP carriage network. Despite the IP focus, Telstra are by no means locking into a single technology within its DMO architecture, but have a requirement to support existing data products and future bit-transport products. They also have a requirement that all processes associated with the network are to be fully automated. To this end, they have chosen a network management strategy that can deal with the diversity and complexity inherent within such requirements.

Management domains built around a hierarchical TMN model have been chosen to build upon the conglomerate environment of manually driven element managers that typically exist today. Under this architecture, domain managers reside on top of traditional element managers and the network, with the responsibility to manage groupings within the network that have common properties. Enterprise requirements determine the nature of the groupings i.e. technology, topology, vendor or business. Above the domain managers exists a cross-domain manager that effectively has an end-to-end network view. Only information relevant to the end-to-end operation of the network is passed from domain managers to the cross-domain manager.

Finally, on top of the cross-domain manager exists a service management layer focused on providing a service view (implicitly end-to-end) rather than a network view to the customer. With all levels of domain management built using distributed object-oriented technologies, Telstra believes this architecture will provide the flexibility and scalability to deal with their management requirements under a DMO. Note that this

includes the telephony network. While initially it will co-exist with the DMO, it will gradually be transitioned to become an application on the DMO.

3.2.2 Use of CORBA

Traditional centralised and hierarchical network management paradigms (e.g. provided by SNMP or CMIP) lack flexibility and robustness. The use of CORBA can greatly improve these features due to [17]:

- Cost-effectiveness for large-scale deployments;
- Platform independence together with a large range of development language mappings;
- Middleware growth within the application domain, use of CORBA provides seamless integration of management interfaces into applications together with a common infrastructure for applications and management;
- Common support and access to CORBA protocols within Web Browser technology.

Management platforms using CORBA include the *Tivoli* TME10 [15] and *HP OpenView* IMSM [16].

However, despite the above advantages, CORBA has a disadvantage in relation to complexity, together with the corresponding expense of implementation. As a result CORBA tends to be used in large-scale deployments and high-end management products. Another area that needs improvement is the access to management information within the CORBA architecture. Currently access to traditional MIBs is achieved through translation procedures or gateways. With the OMG working on facilities & domain interfaces within the telecommunications area, as well as work currently under way within IEEE P1520 in relation to service management, this need is likely to be addressed in the near future. This work should provide open vendor independent interfaces to access management information directly in the CORBA domain. As service management is a relatively new area of focus for managers of networks, there is little existing MIB definitions related to this area. It's in the area of service management that CORBA may have the greatest impact. In the following section we'll examine the trends in this area.

3.2.3 Use of Mobile Code

Network management based on the use of mobile code is a relatively new concept, which, as with CORBA presented in the previous section, aims at providing high flexibility and robustness. This concept enables a Mobile Code System (MCS) to transfer the code of an execution unit or with some approaches, both code and the state

of an execution unit to another host where the execution can be initiated or resumed [36]. Among several different approaches to this concept, two namely Management by Delegation (MbD) and Active Networks, look the most promising. The MbD approach assumes sending a program (called the *delegated agent*) from the client to the server where it is dynamically linked and executed (either immediately or with some delay). This approach has been adopted by the IETF in its recent extensions to SNMPv3.

For the Active Networks approach, nodes in the network can perform: (a) computations on packet contents (and possibly modify them) if the packets carry data; or (b) execution of the packet contents if the packet carries a miniature of a program. The main problems associated with Active Networks are security, performance, and interpretability [36].

3.2.4 Use of the Web

The fundamental drivers of the Internet have lead to development of Web base management architectures, now commonly supported on current management platforms. There are two basic architectural approaches [17]. Firstly, there is an *embedded approach* where HTTP servers are embedded in network resources and HTTP becomes the management protocol facilitating management access via Web browsers. This has the advantage of simplicity and low lost, and is replacing traditional console access to network resources.

Secondly, there is a *proxy approach* whereby existing element managers are simply Web enabled through the addition of a HTTP server. Users may then browse from anywhere on the network, the HTTP-advertised network services of the element manager. This approach protects legacy investments adding flexibility to the user.

There are two areas of standardisation occurring in relation to Web base management architectures. The first relates to the proxy approach and is a Java based standard. Sun together with partners have developed the JMX (Java Management Extensions)[1] [31] that defines a management architecture, Application Procedure Interfaces (APIs), and management services. It is built upon Java component technology, and among its features it facilitates instrumentation of application code and integration of existing management technologies (e.g. SNMP). This architecture has been designed with a service-driven network perspective in mind, and is focused on management integration through common interfaces and a common architectural representation. Recently, Sun announced the first instantiation of this specification with the release of the Java Dynamic Management Kit [32].

The second area relates to an original consortium of manufactures called the WBEM (Web-Based Enterprise Management) [35] initiative. This initiative now forms part of the industry standards body called the DMTF (Distributed Management Task Force). It is focused on realising the power of the Web for management interoperation. The focus

[1] JMX was originally known as JMAPI (Java Management API)

of the WBEM has changed over the years. Originally it targeted work in relation to a new management architecture called hypermedia management (HMM), but after the integration with DMTF the focus was directed more towards development of new management information models. To that end they have developed a data model called the Common Information Model (CIM) [34] that is an implementation independent conceptual information model for describing management. Further to that, they have more recently looked at the issues of mapping CIM to the extensible markup language (XML) (called xmlCIM Encoding specification), and the issues of mapping CIM operations onto HTTP (called CIM Operations over HTTP specification). These specifications highlight the WBEM focus on management integration through the need for common and loss-free management information exchange.

3.3 Service Provision

Service management is rapidly growing in importance. It aims at the quick building and flexible managing of services. In this section, we first present how voice and IP networks support service management, and then describe emerging research and standardisation initiatives to improve service provision.

3.3.1 TINA

The *Telecommunications Information Networking Architecture* (TINA) is probably one of the most widely known conceptual architectures that enable the creation of distributed multimedia services. It tries to integrate the strengths of traditional telecommunications (i.e. high security, reliability and QoS) with the power of users' computers and software capabilities. TINA aims at provisioning any kind of multimedia service, running on a global scale, on different network technologies (e.g. IN, ATM, and the Internet) and any type of connectivity, including multiparty connections.

The *TINA Consortium* (TINA-C) is composed of representatives from almost all major telecommunications players. After a slow start (1990), in 1997 it completed work on an architectural framework, component specifications and feasibility demonstration [18]. In 1998, it started the second phase of the commercial adoption of its architecture. By the year 2000, a large-scale deployment of TINA-conforming products and TINA-based services is expected [19].

The TINA-C main objectives are:

- *Separation of the connectivity software from the switching hardware* – this separation is obtained by using open connection management interfaces and specifying both service and terminal connectivity reference points.
- *Integration of control (signalling) and management* - TINA aims at replacing SS7 and TMN. However, seamless service provisioning for both existing technologies, such

as Intelligent Network and TMN, and new ones like ODP is assumed. Extensive efforts are being made to create mechanisms (e.g. various gateways) to enable smooth transition from old to new technologies. For example, several different approaches have been proposed to enable a smooth TMN to TINA transition [20].

- *Adoption of distributed-objects technology* for the creation of a generic computing and communication platform – TINA follows the OSI *Reference Model of Open Distributed Processing* (RM-ODP). Various controllers, which run on general purpose distributed platforms, exchange information through local and remote invocations. Although these interactions resemble signalling activities, they are expressed in terms of high level operations [21].
- *Support for QoS* - QoS requirements are declaratively specified using the computational and engineering viewpoints (see below);
- *User and service mobility support* – one of the aims is to enable the creation of multimedia services for mobile/wireless users using technologies such as GSM and UMTS.

The *Common Object Request Broker Architecture* (CORBA) is currently used as TINA's *Distributed Processing Environment* (DPE). The use of CORBA provides the means to build robust distributed control and management infrastructure.

3.3.2 IEEE P1520

In 1997, several companies (e.g. Ericsson, DEC) and laboratories initiated a new IEEE standards initiative, called *P1520*, to define a reference model for programmable network interfaces [22]. This model distinguishes several levels (see Fig. 1) composed of entities and separated by programmable interfaces specified in terms of the industry standard *Interface Definition Language* (IDL). The levels correspond to end-user applications, value-added services, network generic services, virtual network devices and network physical elements. Each interface is an *Application Program Interface* (API) open for distributed access. From the viewpoint of this report, there are two important advantages to this model, namely (a) open access to network elements (e.g. switches and routers) by services; and (b) separation of control and management applications from network elements.

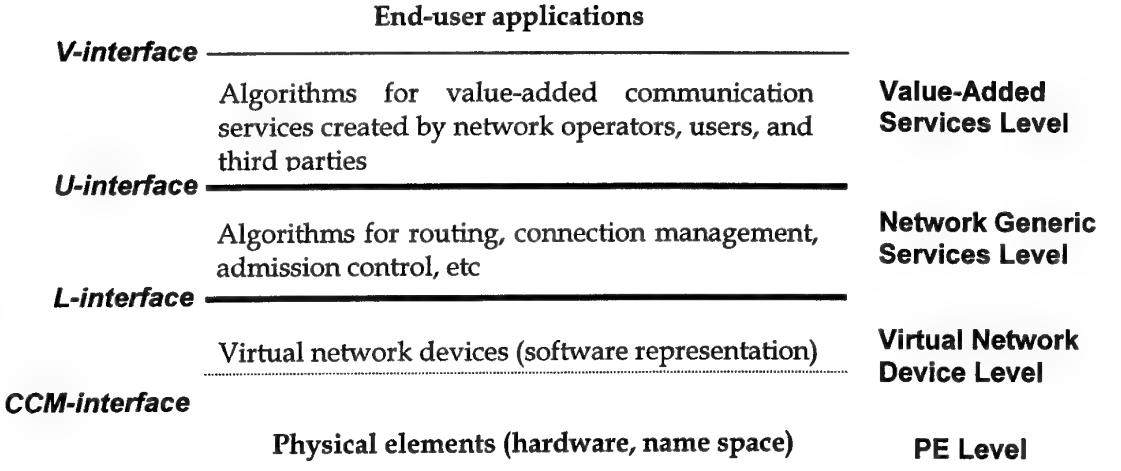


Figure 1. The P1520 reference model

The levels of the model are:

- *Value-Added Services Level* (VASL) - entities at this level are end-to-end algorithms that add value to services provided by lower levels. These algorithms include real-time stream management, synchronisation of multimedia streams etc;
- *Network Generic Services Level* (NGSL) – this level offers (network-wide) generic services to VASL including routing, configuration and admission control. These services are delivered using (distributed) algorithms stored at this level;
- *Virtual Network Device Level* (VNDL) - this level contains entities (objects) that are logical representations (abstractions) of physical elements at the lowest physical level;
    - *Physical Elements* (PE) *Level* – all physical elements of the network reside at this level. These elements are accessed using open protocols. Note that the interface between this level and VNDL is not a programming interface but rather a collection of protocols (e.g. GSMP, CMIP, SNMP).

The P1520 document also suggests the mapping of the proposed interfaces to various types of networks, including ATM, IP (both using routing and switching), SS7 and TINA. As of July 2000, the group was close to delivering full specifications and software for the L interface on ATM switches. While initial work was undertaken, all CCM interface work has been handed over to the IETF General Switch Management Protocol (GSMP) working group. Currently much of the groups focus is directed towards examining interfaces L and U for IP routers and switches.

3.3.3 CORBA extensions to TMN

As mentioned in Section 2.2.1, the TMN is not well suited to model and implement new services in a network. CORBA technology offers a better technology to achieve this purpose [10]. That is why the Joint Inter-Domain Management (JIDM) group has been developing gateways to enable it to perform TMN-like services in CORBA [23].

3.3.4 PARLAY & JAIN

The Parlay consortium [24] specifies an API that abstracts specific telecom and data network capabilities through service (e.g. call control, connection manager, user status) and framework (e.g. authentication, authorisation, auditing, discovery) interfaces which enables secure network-independent access. It addresses an IN like architecture and is specifically targeted at the service provider or those core capabilities application developers looking to value add their product. Its strength revolves around its security management that ensures network integrity is maintained. A second version of this API incorporates IP Network support with QoS access as part of its service manager sub-interface. A user can create virtual provisioned pipes that build upon pre-specified QoS classes offered by the network provider.

Along a similar thread is the Java Advanced Intelligent Networks (JAIN) aimed at building and deploying telecom services through the blending of IN and Internet technologies [25]. This is achieved by offering a framework that exposes functionality within the network for ease of service creation and service delivery. Two sub-groups contribute to this effort. One deals with the low level interfaces into network signaling protocols (IP and SS7 domains), and the second deals with standard and consistent API's exposed as Javabeans to applications for Java service creation (i.e. call control and call processing transactions) utilising the lower layer protocol encapsulations.

An important strength is that it leverages and integrates with other ongoing Java APIs such as the Java Telephone API (JTAPI). This work is considered to be complementary to the Parlay APIs, with ongoing effort to create a Parlay JAIN API specification that provides a Java platform instantiation of the Parlay specification, drawing upon its strengths in relation to secure public access.

3.3.5 Softswitch Consortium

A relatively new consortium worth following in this field of IP service and application management is the Softswitch consortium. "Softswitch" is a name given to applications that emulate circuit switching in software [26]. Generally, the consortium is attempting to advance the formation of open standards and interoperability to support rapid advancement of application development on networks that support both voice and real-time multimedia communications. This consortium is specifically focused on IP network infrastructure. (Note there is a counterpart forum focused on ATM network infrastructure called the Multiservice Switching Forum). Currently, there is a strong

focus on IP voice applications, with *softswitches* considered to be the technologies needed to link traditional and IP networks. Being founded in May 1999, there are no publicly available documents yet.

3.3.6 DMIF

The DMIF (Delivery Multimedia Integration Framework) represents a framework standard defined within the context of the MPEG4 ISO standardisation effort. It represents a significant paradigm shift from traditional frameworks, through the encapsulation of not only control plane functionality, but also the data plane. DMIF supports network transparency through its aim to "allow each delivery technology to be used for its unique characteristics in a way transparent to application developers" [27]. Despite its relationship with MPEG4, DMIF can be considered a standalone specification with applicability to the broader application community [28] (not just IP). In particular (by definition) the open programmable network community. Applications are built on top of, and access the framework, via a semantic API called the DMIF Application Interface (DAI). As part of the second version of this specification, semantics have been included supporting the request, monitoring and renegotiation of network QoS.

3.3.7 IETF COPS/PIBs (policy managers)

The IETF have defined the Common Open Policy Service (COPS) protocol for robust client/server interaction between policy management applications [29]. Broad applicability was seen for this work with the formation of a policy-working group to foster frameworks for policy definition and administration. The aim is to capture in a *Policy Repository* a policy definition, which is generic in the sense that it is independent of specific network mechanisms used to enforce the policy. A *Policy Consumer* translates that generic policy into network device specific requirements and representations, interacting with policy enabled network elements (called *Policy Targets*) that enforce the policy. Policy Targets are not restricted to IP devices only. Recent IETF drafts [30,31] have proposed refinements to the generic models needed to represent QoS policy information within the framework.

4. Conclusions

This report has briefly presented current and emerging approaches to Network Management and Service Provision in both voice and data public carrier networks.

The report has stressed the importance of the trend toward joining separated voice and data public networks belonging to a single carrier into an integrated telecommunications infrastructure to provide highly innovative product packages. This convergence, together with the deregulated telecommunications environment that is opening up service provisioning to third parties, is leading to increased complexity

of network management. As a result we are seeing a clear direction in the use of layered management architectures (e.g, the one proposed for Telstra's Data Mode of Operation). Additional to this complexity, there is a corresponding staggering cost increase associated with network management. This requires the development of management architectures that are highly flexible and potentially highly automated. Middleware, active network and Web based technologies are being used to address these issues. The ever growing demand for new sophisticated services involving a variety of media, and at the same time the need for rapid service provisioning, have resulted in service-centric oriented approaches to network management. One important feature of this trend is the provision of more service control to end-users. Together with the already mentioned opening up of service provisioning to third parties, this has triggered intensive research and standardisation efforts on new service management architectures, including open Application Procedure Interfaces (APIs). While still in its infancy, some of the more promising approaches in this direction have been presented in this report.

A number of new approaches and directions are emerging on how networks will be managed, however they are not necessarily in competition. Rather they tend to be addressing different aspects of network management.

5. References

1. ITU-T Recommendation M.3010, "Principles for a Telecommunications Management Network", July 1996.
2. K. Johannessen, "Security of TMN", IEEE Network Operations and Management Symposium, Kyoto, Japan, 1996.
3. J. Martin-Flatin, S. Znaty, "A Simple Topology of Distributed Management Paradigms", Proceedings of Distributed Systems Operations and Management (DSOM) conference, Sydney, Oct. 1997.
4. D. S. Sidor, "TMN Standards: Satysfying Today's Needs While Preparing for Tomorrow", IEEE Communications Magazine, March 1998.
5. Frye R, Levi D, Routhier S, Wijnen B, "Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework)", Proposed Standard RFC 2576, March 2000.
6. W. Stallings, "SNMP anbd SNMPv2: The Infrastructure for Network Management", IEEE Communications Magazine, March 1998.
7. Blumenthal, U. and Wijnen, B., "The User-Based Security Model for Version 3 of the Simple Network Management Protocol (SNMP)", RFC 2574, May 1999.
8. Wijnen, B., Presuhn, R. and K. McCloghrie, "View-based Access Control Model for the Simple Network Management Protocol (SNMP)", RFC 2575, May 1999.

9. "Telecommunications Network Management - Technologies and Implementations", S. Aidarous, T. Plevyak (Editors), IEEE Press, New York, 1998.

10. Q. Kong, G. Chen (1996), 'Integrating CORBA and TMN Environments', IEEE Network Operations and Management Symposium, Kyoto, Japan.

11. A. Dittrich, M. Hoft, "Integration of a TMN-based Management Platform into a CORBA-based Environment", IEEE Network Operations and Management Symposium, Kyoto, Japan, 1996.

12. Jong-Tae Park, Su-Ho Ha, "Design and Implementation of CORBA-based TMN SMK System", IEEE Network Operations and Management Symposium, Kyoto, Japan, 1996.

13. S. Rahkila, S. Stenberg, "Experiences on Building a Distributed Computing Platform Prototype for Telecom Network and Service Management", 5th IFIP Intern. Symposium on Integrated Network Management, USA, 1997.

14. D. Giddy, "Towards a Data Mode of Operation - Telstra's DMO Project", Telecommunication Journal of Australia, Vol 49, No. 4, 1999.

15. Tivoli home web page, http://www.tivoli.com/

16. HP Integrated Multi-Service Management Web Page, http://www.hp.com/ovc/catalyst.htm

17. H Hegering, S. Abeck, B. Neumair, "Integrated Management of Networked Systems", Morgan Kaufmann Publishers Inc., 1999.

18. Y. Inoue, D. Guha, H. Berndt, "The TINA Consortium", IEEE Communications Magazine, Sept. 1998.

19. "TINA Consortium delivers software architecture for advanced multimedia networking", TINA-C Press Release, Santiago de Chile, Nov. 1998. http://www.tinac.com/TINA2000/press/deliver.html

20. J. Pavo, J. Thomas, Y. Bardout, L. Hauw, "Management in the TINA Framework", Communications Magazine, March 1998.

21. A. Lazar, "Programming Telecommunication Networks", in "Building QoS into Distributed Systems" A. Campbell & K. Nehrstedt (Editors), IFIP, published by Chapman & Hall, 1997.

22. P1520, "Application Programming Interfaces for Networks", IEEE Draft White Paper, 1998.

23. Joint Inter-Domain Management (JIDM) group, http://www.jidm.org/

24. The Parlay Group Web page http://www.parlay.org/

25. "JAIN: Integrated Network APIs for the Java Platform", June 1999, http://java.sun.com/products/jain/

26. Softswitch Consortium Web Page http://www.softswitch.org/

27. ISO/IEC JTC1/SC29/WG11 N2506, "Information technology - Coding of audio-visual objects - Part 6: Delivery Multimedia Integration Framework (DMIF)", ISO/IEC 14496-6:1999

28. ISO/IEC JTC1/SC29/WG11 N2313, "DMIF FAQ", Delivery Sub-Working Group, July 1998, http://drogo.cselt.stet.it/mpeg/faq/faq-dmif.htm

29. Reichmeyer, F. et al. (2000), 'COPS Usage for Policy Provisioning', work in progress, draft-ietf-rap-pr-02.txt , March.

30. Snir Y, Ramberg Y, Strassner J, Cohen R (2000), 'Policy Framework QoS Information Model', work in progress, draft-ietf-policy-qos-info-model-00.txt, January.

31. Snir Y, Ramberg Y, Strassner J, Cohen R (2000), 'QoS Policy Schema', work in progress, draft-ietf-policy-qos-schema-00.txt, February.

32. SUN Microsystems, "JAVA Dynamic Management Kit White Paper", April 2000, http://www.sun.com/software/java-dynamic/whitepapers.html

33. SUN Microsystems, "JAVA Management Extensions White Paper", Dec 1999 http://java.sun.com/products/Java/Management/wp/

34. DMTF Web Page, "CIM Standards", http://www.dmtf.org/spec/cims.html

35. DMTF Web Page, "WBEM Standards", http://www.dmtf.org/spec/wbem.htmlMartin-Flatin J, Znaty S, 'Two Taxonomies of Distributed Network and Systems Management Paradigms', in 'Emerging Trends and Challenges in Network Management', Ho L. and Ray P. (Eds.), Plenum Publishers, 2000

DISTRIBUTION LIST

IP Convergence in Global Telecommunications

-

New Approaches to Network Management and Service Provision

Marek Kwiatkowski and Peter George

AUSTRALIA

DEFENCE ORGANISATION

Task Sponsor

Director General C3I Development
DCD
DOISD
PD JP 2047 (CWAN)
PD JP 2068 (NOC)
PD JP 2061 (EXC3ITE)

S&T Program

Chief Defence Scientist
FAS Science Policy } shared copy
AS Science Corporate Management
Director General Science Policy Development
Counsellor Defence Science, London (Doc Data Sheet)
Counsellor Defence Science, Washington (Doc Data Sheet)
Scientific Adviser to MRDC Thailand (Doc Data Sheet)
Scientific Adviser Policy and Command
Navy Scientific Adviser (Doc Data Sheet and distribution list only)
Scientific Adviser - Army (Doc Data Sheet and distribution list only)
Air Force Scientific Adviser
Director Trials

Aeronautical and Maritime Research Laboratory

Director

Electronics and Surveillance Research Laboratory

Director

Chief of Communications Division
Research Leader Military Information Networks
Head Network Requirements
Head Network Architecture
Head Wireless Systems
Research Leader Secure Communications
Head Intelligent Networks
Research Leader Military Computing Systems Branch
Marek Kwiatkowski
Peter George

DSTO Library and Archives

Library Fishermans Bend (Doc Data sheet only)
Library Maribyrnong (Doc Data sheet only)
Library Salisbury (1 copy)
Australian Archives
Library, MOD, Pyrmont (Doc Data sheet only)
Library, MOD, HMAS Stirling

US Defense Technical Information Center, 2 copies
UK Defence Research Information Centre, 2 copies
Canada Defence Scientific Information Service, 1 copy
NZ Defence Information Centre, 1 copy
National Library of Australia, 1 copy

Capability Development Division

Director General Maritime Development (Doc Data Sheet only)
Director General Aerospace Development (Doc Data Sheet only)

Navy

SO (Science), Director of Naval Warfare, Maritime Headquarters Annex, Garden Island, NSW 2000. (Doc Data Sheet only)

Army

ABCA Standardisation Officer, Puckapunyal, (4 copies)
SO (Science), DJFHQ(L), MILPO Enoggera, Queensland 4051 (Doc Data Sheet only)
NAPOC QWG Engineer NBCD c/- DENGRS-A, HQ Engineer Centre Liverpool Military Area, NSW 2174 (Doc Data Sheet only)

Intelligence Program

DGSTA Defence Intelligence Organisation
Manager, Information Centre, DIO

Defence Information Systems

DGIS-DIS
DGCIPP-DIS
D-DISC

Corporate Support Program

Library Manager, DLS Canberra

UNIVERSITIES AND COLLEGES

Australian Defence Force Academy
Library
Head of Aerospace and Mechanical Engineering
Serials Section (M list), Deakin University Library, Geelong, 3217
Senior Librarian, Hargrave Library, Monash University

Librarian, Flinders University

OTHER ORGANISATIONS

NASA (Canberra)
AusInfo
State Library of South Australia
Parliamentary Library, South Australia

OUTSIDE AUSTRALIA

ABSTRACTING AND INFORMATION ORGANISATIONS

Library, Chemical Abstracts Reference Service
Engineering Societies Library, US
Materials Information, Cambridge Scientific Abstracts, US
Documents Librarian, The Center for Research Libraries, US

INFORMATION EXCHANGE AGREEMENT PARTNERS

Acquisitions Unit, Science Reference and Information Service, UK
Library - Exchange Desk, National Institute of Standards and Technology, US

SPARES (5 copies)

Total number of copies: **63**

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION
DOCUMENT CONTROL DATA

1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE

Report Series on the Adoption of Internet Protocols in Public Carrier Networks
-
New Approaches to Network Management and Service Provisionings

3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION)

Document	U
Title	U
Abstract	U

4. AUTHOR(S)

Peter George and Marek Kwiatkowski

5. CORPORATE AUTHOR

Electronics and Surveillance Research Laboratory
PO Box 1500
Salisbury SA 5108 Australia

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO-TR-1075	AR-011-645	Technical Report	November 2000

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. NO. OF PAGES	12. NO. OF REFERENCES
E8709/007/0016/01(U)	JNT 99/150	DGC3ID	16	31

13. URL ON WORLD WIDE WEB
http://www.dsto.defence.gov.au/corporate/reports/DSTO-TR-1075.pdf

14. RELEASE AUTHORITY

Chief, Communications Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for public release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, SALISBURY, SA 5108

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CASUAL ANNOUNCEMENT Yes

18. DEFTEST DESCRIPTORS

Computer networks, Internet, Communications networks

19. ABSTRACT

This report overviews current and emerging approaches to network management and service provision in both voice and IP data public carrier networks. These two functions are described for the traditional infrastructure, where voice and data networks are separated, and when these networks are interconnected; the latter being an emerging trend.